



# **TASK ORDER (TO)**

**47QFCA20F0023**

## **Technical & Acquisition Services Support (TASS)**

in support of:

## **Remote Sensing Center – National Capital Region (RSC-NCR)**

**Issued to:**

**Apogee Engineering, LLC  
8610 Explorer Dr. Suite 305  
Colorado Springs, CO 80920**

**Issued under:**

**GSA's One Acquisition Solution for Integrated Services (OASIS Small Business)  
Indefinite-Delivery Indefinite Quantity (IDIQ) Contract  
Conducted under Federal Acquisition Regulation (FAR) 16.505(b)(1)  
Original Award: September 29, 2019**

**Administrative Continuance to:**

**The Federal Systems Integration and Management Center (FEDSIM)  
1800 F Street, NW (QF0B)  
Washington, D.C. 20405  
July 10, 2020**

September 1, 2020

**Technical & Acquisition Services Support (TASS)**

**Mission Partner: Remote Sensing Center (RSC) – National Capital Region (NCR)**

**Type: Time & Materials (T&M)**

**Background:** The Remote Sensing Center (RSC) is an interdisciplinary research group chartered under the Dean of Research at the Naval Postgraduate School (NPS). The RSC office in the National Capital Region (RSC-NCR) interacts with Department of Defense (DoD), Intelligence Community (IC), and other U.S. Government mission partners to understand their requirements, discover cutting-edge technologies (in Government, commercial, academic, and non-profit sectors), and bring real-world examples to NPS for enhanced training, education, thesis focus, and application as well as viable and unique solutions to the remote sensing community. In parallel, the RSC-NCR also brings technical and programmatic expertise together to allow DoD and IC mission partners to achieve their mission. The majority of supported projects involve emerging or future needs that require forward-looking and quick-reaction capabilities. The RSC-NCR is a mission-enabler with the tools and skill sets to support needs at the tempo they emerge. In addition, RSC-NCR supports research, programmatic, and execution effort with DoD and IC mission partners.

**Period of Performance (PoP):**

- Base Period: 3/1/2020 – 09/28/2020
- Option Period 1: 09/29/2020 – 09/28/2021
- Option Period 2: 09/29/2021 – 09/28/2022
- Option Period 3: 09/29/2022 – 09/28/2023
- Option Period 4: 09/29/2023 – 09/28/2024

**1.0 Scope and Tasks:**

The purpose of this requirement is to obtain technical expertise services. Contractor responsibilities shall focus on program management, financial and budget support, mission partner support, technical advisory support, and technology and capability demonstration support. Support services shall also include option to provide increased technical support for mission partner contracts focused on Intelligence, surveillance, and reconnaissance (ISR) logistics and cyber support.

In particular, the contractor shall provide personnel with the expertise to develop and coordinate concepts and requirements for the application of current and emerging technologies as they apply to DoD missions. Furthermore, the contractor shall provide a support team that has a thorough knowledge of the DoD customer base and possesses the capability to support the objectives outlined in this Performance Work Statement (PWS).

**1.1 Program Management Task:**

1.1.1 The contractor shall assist in the development of program briefings, schedules, and budgets. As required, the contractor shall provide monthly status report and planning documentation to the Contracting Officer's Representative (COR).

1.1.2 The contractor shall assist in strategic planning and execution of various DoD missions. The contractor shall develop technology roadmaps, risk management plans, and strategies to support programmatic decisions relative to RSC-NCR mission objectives.

1.1.3 The contractor shall document travel executed in support of requirements, meetings and interactions with customers, partners and other key organizations.

1.1.4 The contractor shall provide technical support for classified and unclassified programs; attend kickoff meetings, reviews, planning sessions/meetings, test events, demonstrations, and out-brief meetings; develop, maintain, and monitor metrics for program execution oversight; ensure that milestones and deliverables are accomplished on schedule; coordinate training and transition efforts; and, provide technical support for transition efforts.

1.1.5 The contractor shall visit combatant command (COCOMs), Armed Services, Department of Energy (DOE), Department of Homeland Security (DHS), other governmental agencies (OGA), and IC installations for meetings, briefings, and reviews of relevant topics. In support of interagency objectives, the contractor shall coordinate with other agencies to ensure that development efforts are coordinated and non-duplicative, meeting the objectives of all stakeholders, and leveraging developmental efforts internal and external to DoD to maximize return on DoD investments.

1.1.6 The contractor shall provide support services and technical expertise for RSC-NCR research projects and programs. This shall include monitoring of financial resources, project funding and expiration dates, development and monitoring of project Plan of Action and Milestones (POA&M), schedule oversight, attendance at in-process reviews, out-briefs, etc., identification of and interaction with final transition partners, and technical oversight of all other contractual portions of programs. The contractor shall assist in coordinating multi-agency, multi department investments to ensure resources are available and synergies in entity interests are maintained. The contractor shall monitor progress on performance metrics for all acquisition efforts.

1.1.7 The contractor shall provide contract management support services and advise the COR on the Federal Acquisition Regulations (FAR), baseline management, and project control post award. The contractor shall provide support personnel with extensive knowledge of Government business practices, contract and procurement management, program management, Federal compliance requirements, and contract management.

1.1.8 The contractor shall perform analysis of deliverables, requirements, compliance, budgeting, work breakdown structure, cost variance analysis, forecasting, and integrate schedules across applicable projects. The contractor shall work with partners in coordinating multi-agency, multi-department investments to ensure resources are available and synergies in mission partner interests are maintained.

1.1.9 The contractor shall assist in all areas of programmatic support, drafting and amending briefs, responses, documents and reports; drafting, developing, and reviewing annual reviews and program status reports; drafting, developing, and reviewing Future Years Defense Program (FYDP) and Program Objective Memorandums (POM) inputs and plans; and addressing

Congressional submissions, Freedom of Information Act (FOIA) requests, and other required documentation.

## **1.2 Financial and Budget Support:**

1.2.1 The Contractor shall support the COR in providing financial support services and technical expertise for RSC-NCR research projects and programs. This shall include monitoring of financial resources, project funding and expiration dates, development and monitoring of project Plan of Action and Milestones (POA&M), schedule oversight, attendance at in-process reviews, out-briefs, etc., and identification of and interaction with final transition partners. The contractor shall assist in coordinating multi-agency, multi department investments to ensure resources are available and synergies in entity interests are maintained.

1.2.3 The contractor shall provide initial budgetary products and updates to draft existing President's/Office of the Secretary of Defense (OSD)/ Financial Management and Budget (FMB) budget exhibits. The contractor shall generate, update, and draft budgetary reclaims and impact statements. The contractor shall prepare Issue Papers in support of budget data calls. The contractor shall support the DoD customer in the following activities: defend budgets; respond to OSD budget review questions; conduct what-if drills, plus- ups and supplements; respond to Congressional request for information; and prepare briefings. The contractor shall prepare initial execution data, analysis and updates execution data calls, mid-year and program review documentation.

1.2.4 The contractor shall populate and maintain "real time data" in corporate financial databases. The contractor shall assist in the preparation of life cycle cost analysis/total ownership cost analysis, cost benefit analysis, cost comparison analysis, business case analysis, trade-studies, analysis of alternatives, and cost as an independent variable analysis.

## **1.3 Mission Partner Support:**

1.3.1 The Contractor shall coordinate with COCOMs, Armed Services, DOE, DHS, Department of State, and IC organizations with or without DoD Government representatives for meetings, briefings, and reviews of relevant topics.

1.3.2 In support of the DoD customer's interagency objectives, the contractor shall coordinate with other agencies to ensure that development efforts are coordinated and non-duplicative, meeting the objectives of all stakeholders, and leveraging developmental efforts internal and external to DoD to maximize return on DoD investments.

1.3.3 The contractor shall attend and assist DoD in hosting symposia, workshops, and conferences on operational, scientific, and technology topics.

1.3.4 The contractor shall attend DoD customer meetings and participate in pertinent conferences and forums in addition to specific DoD customer projects. The contractor shall

participate and organize intra and interagency workshops and working group meetings related to research projects as directed by the DoD customer.

1.3.5 The contractor shall assist the DoD customer in scheduling, supporting, and hosting meetings, workshops, and conferences. The contractor shall attend DoD customer workshops, meetings, conferences and symposia as requested.

#### **1.4 Technical Advisory Support:**

1.4.1 The Contractor shall provide personnel with extensive technical and programmatic experience covering a wide-range of technical and programmatic disciplines, to include (but limited to): materials; sensing technologies, to include active and passive optical, infrared (IR), Overhead Persistent Infrared (OPIR), multispectral (MSI), hyperspectral (HSI), Light Detection and Ranging (LIDAR), (Radio Detection And Ranging) (RADAR), acoustic, magnetic, Signals Intelligence (SIGINT), nuclear, chemical, and other sensors; power sources, processing, exploitation and dissemination (PED) of Intelligence, Surveillance and Reconnaissance (ISR) data; communications; aerospace; biometrics; human performance factors; medical factors; special operations forces (SOF); full motion video (FMV) processing; wide area motion imagery (WAMI) collection and processing; computational fluid dynamics; aircraft/missile performance; directed/kinetic energy weapons; space superiority; and national security policy.

1.4.2 The contractor shall provide scientific and engineering expertise and advice in support of requirements analysis, operational needs determinations, technical systems application evaluations, and science and technology planning and critiques.

1.4.3 The contractor shall evaluate the applicability of newly developed, evolving, and emerging technical capabilities to fulfill DoD current and future technology requirements and assess the potential technology viability based on underlying scientific phenomenology.

1.4.4 The contractor shall attend DoD on Integrated Product Teams (IPTs) and participate in pertinent conferences and forums. The contractor shall assist the DoD customer in assessing technology proposals, both for technologies and for technology demonstrations, submitted to the DoD customer or to partnering organizations with similar or congruent technical objectives. The contractor shall evaluate the possible applications for technologies, the alternatives that might be viable, the cost and risks of the proposed solutions, the suitability of the proposed performance metrics, and the schedule to achieve the solutions. The contractor shall recommend proposal changes to maximize support potential and value to the Government.

1.4.5 To ensure that generated capabilities accurately satisfy mission needs, the contractor shall assist in engaging users in candidate solutions, determine training needs and costs, and assess the operational limitations of proposed solutions. The contractor shall develop a mechanism to evaluate/assess capabilities and ensure that each capability is assessed and the summary of the

capability and its ratings is documented and shared with the DoD customer in a consistent and searchable manner.

1.4.6 The contractor shall support the DoD in the identification of critical operational needs and identify, prioritize, and recommend candidate solutions for key gaps, shortfalls and operational needs in support of DoD efforts.

1.4.7 The contractor shall provide support services for special studies, analyses, and reviews for specified mission area needs for emergent work requirements encountered in the performance of and within the scope of this PWS. These activities may include, but are not limited to research and analysis involving specialized expertise in the areas of collection management planning, indications and warning/anticipatory intelligence, imagery and geospatial analysis, signals intelligence analysis, cyber operations, perception management strategies, exercises, and war games. Specialized technical expertise involving analysis of space protection strategies, concepts, cyber security policy, and intelligence of foreign threats shall be provided.

1.4.8 The contractor shall perform mission need and analysis assessments of specific adversary nations' military capabilities, infrastructure, economy, culture, decision processes, strategic objectives, key decision makers, future military programs, and research and development. Relevant analysis shall be conducted on regional factors in all of these areas, to include a vulnerability analysis of all factors to demonstrate what key targets can be affected by the application of US power. The contractor shall analyze available capabilities to determine which capabilities (or combination of capabilities) can be used to affect adversary vulnerabilities. This analysis will cross all functional areas in DoD, consider all instruments of national power (diplomatic, informational, military and economic), will consider capabilities that can be employed during all phases of conflict, and will consider capabilities protected as Special Compartmented Information (SCI), Special Access Programs (SAP), and Alternate Compensatory Control Measures (ACCM). This analysis will also result in a capabilities gap analysis that will highlight those vulnerabilities that the US cannot affect with current capabilities. Where applicable, the contractor's analysis shall comply with the Joint Capabilities Integration and Development System (JCID) process for the future integration into the system or force.

## **1.5 Technology and Capability Demonstration Support:**

1.5.1 The contractor shall demonstrate emerging capabilities for LIDAR including topographic surveys/collection, analysis of waveform data, and data delivery and processing (e.g., point cloud, full waveform). As required, the contractor shall provide a Technical Capability Report of each demonstration to the COR. Contractor may be required to purchase software and/or

software licenses.

1.5.2 The contractor shall demonstrate capabilities for subsurface acoustics including CONUS and/or OCONUS field testing of 3D directional sensors rated up to 1000 meters and advanced exploitation and processing of collected data. As required, the contractor shall provide a Technical Capability Report of each demonstration to the COR. Contractor may be required to purchase software and/or software licenses.

1.5.3 The contractor shall demonstrate cyber security capabilities through commercial solutions, such as display of threats in real time, critical infrastructure service delivery, mobile device authentication and securitization, and risk assessment and mitigation. As required, the contractor shall provide a Technical Capability Report of each demonstration to the COR. Contractor may be required to purchase software and/or software licenses.

### **1.6 Monthly Report/Monthly Meeting:**

Contractor will submit a monthly status report and conduct a monthly progress review call with the COR. The contractor will provide an agenda and teleconference line for monthly meetings across stakeholders. Topics during meeting will include progress, risks and issues, and interim recommendations. Monthly status report will include milestone progress, risks and issues, and financial reporting.

### **1.7 Key Personnel:**

The following are the three (3) personnel who shall be designated as “Key.” The Government does not intend to dictate the composition of the ideal team to perform this Task Order (TO):

- a. One (1) Project Manager (PM)
- b. One (1) Engineer
- c. One (1) Senior (Sr.) Engineer

It is required that the PM has the following qualifications:

More than five (5) years of experience with the RSC mission.

- At least ten (10) years of experience leading studies and analysis teams.
- Has or is eligible for a Top Secret / Special Compartmented Information / Special Access Program (TS/SCI/SAP) clearance with a current background investigation.
- Bachelor’s Degree in Business or Engineering

It is desired that the PM has the following qualifications:

- Expertise in strategic planning; technology assessment & transition; and strategy/business development.
- Professional Project Management Certification (PMP)
- Has a Top Secret / Special Compartmented Information / Special Access Program (TS/SCI/SAP) clearance with a current background investigation.
- Master's Degree in Business or Engineering

It is required that the Engineer has the following qualifications:

- More than three (3) years of experience with the RSC mission.
- Has or is eligible for a Top Secret / Special Compartmented Information / Special Access Program (TS/SCI/SAP) clearance with a current background investigation.
- Bachelor's Degree in Engineering

It is desired that the Engineer has the following qualifications:

- Experience in cyber security/systems; emerging technology, technology assessment, ISR and DoD/IC operational needs.
- Has a Top Secret / Special Compartmented Information / Special Access Program (TS/SCI/SAP) clearance with a current background investigation.

It is required that the Sr. Engineer has the following qualifications:

- More than five (5) years of experience with the RSC mission.
- At least ten (10) years of experience in advance technology.
- Has or is eligible for a Top Secret / Special Compartmented Information / Special Access Program (TS/SCI/SAP) clearance with a current background investigation.
- Bachelor's Degree in Engineering or Technology

It is desired that the Sr. Engineer has the following qualifications:

- Has a Top Secret / Special Compartmented Information / Special Access Program (TS/SCI/SAP) clearance with a current background investigation.
- Expertise in cyber security/systems; emerging technology; technology innovation; machine-to-machine and IoT networks; and data analytics
- Master's Degree in Engineering or Technology

The Government desires that Key Personnel be assigned full-time for the duration of the TO. Other personnel shall be assigned on a full-time or part-time as needed.

#### **1.7.1 Key Personnel Substitution:**

The contractor shall not replace any personnel designated as Key Personnel without the written concurrence of the COR. Prior to utilizing other than the Key Personnel specified in its proposal in response to the solicitation, the contractor shall notify the COR of the existing TO. This notification shall be no later than ten calendar days in advance of any proposed substitution and shall include justification (including resume(s) and labor category of proposed



substitution(s)) in sufficient detail to permit evaluation of the impact on TO performance. Substitute Key Personnel qualifications shall be equal to, or greater than, those of the Key Personnel substituted. If the COR determine that a proposed substitute Key Personnel is unacceptable, or that the reduction of effort would be so substantial as to impair the successful performance of the work under the TO, the contractor may be subject to default action as prescribed by FAR 52.249-8, Default.

### **1.7.2 Optional Support Option**

The Government may execute optional support options during the course of the contract to increase manpower levels for the tasks listed in this PWS. Exercising these options will be dependent on a level of work determination made by the government each year. The Government will notify the contractor prior to exercising these options to allow ample time for the contractor to obtain the required personnel.

### **2.0 Deliverables:**

The contractor shall develop and maintain an efficient and effective quality control program to ensure conformance to contractual requirements. A draft comprehensive written Quality Control Plan (QCP) shall be submitted at time of proposal. A final QCP shall be submitted to the Contracting Officer via GSA ASSIST, fifteen (15) days following the start of contract performance period. If changes are made thereafter, the COR will approve or disapprove changes within fifteen (15) work days after receipt. If the submission is disapproved, the contractor shall submit a revised Quality Control Plan within five (5) working days after disapproval. The Quality Control Plan shall address Best Practices, Service Assurance, and the attached Quality Assurance Surveillance Plan (QASP). The Government's QASP for this requirement is shown in Attachment 02.

For example, a QCP shall contain, at a minimum:

- General provisions including objectives and scope of contractor's Quality Control (QC) Program.
- Descriptions of contractor's QA program organization, participants, and their roles and responsibilities.
- Detailed descriptions of the customer's quality system requirements including but not limited to: document control, records management, QA and Quality Control (QC) and procurement of key items and services (e.g., reagents), corrective action, traceability, audits and inspections, and QA reporting to the Government.

**QUALITY ASSURANCE SURVEILLANCE:** The Government will monitor the contractor's performance through the use of a Quality Assurance Surveillance Plan (QASP), in accordance with the Performance Requirements Summary in the task order. The Government reserves the right to review services to be provided, including those developed or performed at the contractor's facilities, to determine conformance with performance and technical requirements. Government quality assurance will be conducted on behalf of the Contracting Officer. The COR will be appointed to coordinate the overall quality assurance of technical compliance. Performance feedback shall be provided as required and reported annually in a Contractor Performance Assessment Report (CPAR).

All Deliverable shall be submitted to the COR, with a transmittal letter to the Contracting Officer (CO).

Deliverable ID#	Title	Frequency	Description
2.1	Progress Report	Monthly – Within 5 Business days from start of month	Monthly Contractor Progress, Status, and Management Report (CDRL 001) which provides a current status and the program schedule. This report shall be provided using contractor format. Monthly reports shall be submitted in months where technical effort is expended. (1.1.1)
2.2	Travel Trip Report	Within 5 business days after a trip is completed	Travel Trip Report (CDRL 002) will document the results of each trip and any progress or issues toward the mission outcomes (4.0)
2.3	Quality Control Plan	30 days after award and updated as needed throughout	Per Contract requirements (2.0)
2.4	Technology Transition Report	At end of contract and as directed by COR	Report detailing technology transfer opportunities based on collaboration with mission partners and program on-ramp milestones
2.5	Technical / Capability Reports	At end of technology / capability demonstrations	Report test and evaluation results (1.5)

### 3.0 Place of Performance:

Contractor personnel shall conduct classified and unclassified work in USG CONUS and OCONUS facilities to include Arlington, VA; Honolulu, HI; Monterey, CA; Rome, NY; and Stuttgart, Germany; and unclassified work at contractor CONUS and OCONUS facilities to include (but not limited to) the National Capital Region (NCR); Northeast (e.g., MA, NY); Northern and Southern California; Southwest Border Region (e.g., AZ, NM, TX); Mountain-West (e.g., CO, NV, UT); Hawaii; and Pacific Northwest (e.g., OR, WA).

### 4.0 Travel:

Travel is anticipated during the performance of this work assignment.

The contractor is expected to travel in support of this PWS to various CONUS and OCONUS locations that shall be determined and specified by the COR including but not limited to Arlington, VA; Baltimore, MD; Boston, MA; Brussels, Belgium; Buenos Aires, Argentina; Colorado Springs, CO; Denver, CO; Djibouti, Eritrea; Entebbe, Uganda; Fayetteville, NC; Honolulu, HI; London, United Kingdom; Los Angeles, CA; Monterey, CA; New York, NY; Omaha, NE; Rio de Janeiro, Brazil; Rome, NY; San Diego, CA; San Francisco, CA; San Jose,

CA; Sao Paulo, Brazil; Seattle, Washington; Stuttgart, Germany; Tampa, FL; Tokyo, Japan; Washington, DC; and other locations.

The contractor shall obtain approval from the Contracting Officer through the Contracting Officer's Representative (COR) for all reimbursable travel prior to incurring costs. The contractor will make every effort to make requests a minimum of 2-weeks prior to travel and will provide estimated travel costs as part of the request.

Travel will be reimbursed in accordance with FAR 31.205-46.

The contractor will visit CONUS and OCONUS Government sites, test sites, and other locations as directed by the COR. The number of trips and personnel traveling will be limited to the minimum required to accomplish work. Travel shall be scheduled during normal duty hours whenever possible.

#### **5.0 Government Furnished Equipment (GFE)/Government Furnished Property (GFP):**

For work conducted at Government facilities, the Government shall provide access to Government controlled facilities, equipment, and materials for daily business use, as required for this order. This shall include office space, desk, chair, telephone, internet, computer, shared printer, and requisite consumable materials.

#### **6.0 Security:**

6.1 Clearances: All personnel working on classified projects must be able to obtain a Top Secret Security Clearance, based on a Single Scope Background Investigation (SSBI) or Periodic Review (PR) for Top Secret without complications. Investigations will be completed within at least five years to allow for access to Top Secret level and for access to Sensitive Compartmented Information (SCI) and/or Special Access Program (SAP). Determination of accesses will be dictated by individual task order negotiations. Contractor personnel identified to support a tasking shall be proposed to the PM/COR for review and approval prior to commencing work, and the contractor shall be responsible for obtaining the proper security clearances for its employees. Personnel Security requirements will be IAW DCID 6/4 and/or the NISPOM, as applicable. Special requirements may be established by the Government Program Office responsible of any SAP. The Contractor Program Security Officer (CPSO) supporting an SAP will be certified within the first year of contract commencement as a CPSO. When the period of performance is complete and/or contractor personnel leave work on the project, they will have five (5) days to terminate all their network user accounts, return facility identification badges and all access and courier cards provided by the government.

6.2 Information Security: The contractor shall not divulge any program information related to PWS performance, objectives, files, data, processing activities/functions, user identifications, or other knowledge that may be gained, to anyone who is not authorized to have access to such information. All technical documentation and data exchanged between the Contractor and the Government shall be protected from public disclosure in accordance with the markings contained thereon (i.e. classified in accordance with appropriate DoD and AFRL approved security classification directives and guides). Contractor personnel shall abide by all Government information security rules, procedures, and standards of conduct.

6.3 Physical Security: The contractor shall be responsible for safeguarding all Government property provided for contractor use. At the end of each work period, all Government facilities, equipment, and materials shall be secured. Additionally, the contractor will be required to adhere to established computer security procedures. Physical security requirements will be IAW DCID 6/9 and/or the NISPOM as applicable. All classified work performed for each individual task by the Contractor will be performed for Top Secret/Sensitive Compartmented Information (TS/SCI) and/or Top Secret/Special Access Program (TS/SAP) level at an approved government and/or contractor facility determined by the PM/COR. The contractor location will require Industrial safeguarding at the Collateral Top Secret level and must maintain a Sensitive Compartmented Information (SCIF) and/or Special Access Program Facility (SAPF) for SCI/SAP storage. Program Management support will be performed at a government designated facility. Secure facilities of performance will be identified to the SSO and PM/COR for consideration and appropriately annotated on the DD Form 254 once accreditation determinations have been made by the necessary CSA prior to use.

6.4 Computer Security: For any computer systems for which the contractor is responsible, computer security requirements must be implemented IAW DCID 6/3 and Chapter 8 of the NISPOM. Contractor is authorized use of the NIPRNET, SIPRNET, JWICS and other systems/networks identified on each individual task, but only after prior coordination/approval from PM/COR of system accounts with appropriate accreditations.

6.5 National Agency Checks (NACs): Will be conducted, at a minimum, for all personnel, even if a contractor employee does not require access to classified information in performance of a task order; access to U.S. Government automated information system resources that process sensitive, unclassified, or Privacy Act information may be required. NACs will be conducted in accordance with DoD 5200.2-R. The contractor shall establish and administer personnel and physical security programs in accordance with DoD 5200.2-R and DoD/mission partner physical security criteria.

6.6 DoD Installation Access: The contractor shall comply with the instructions in this section. For the purpose of these instructions, the Servicing Security Activity (SSA) is the local military security organization that provides security support for all Government and contractor personnel performing on the installation.

6.7 Facility Clearance, Personnel Security Clearances, and Background Investigations: The Contractor must possess a facility clearance at the classification level indicated on the associated DD Form 254, Department of Defense (DoD) Contract Security Classification Specification.

6.8 Long-term Visitor Group Security Agreement: The contractor shall comply with the provisions of the National Industrial Security Program Operating Manual (NISPOM), the security procedures of the host military/government/contractor installation where TO performance will occur, and the requirements specified in the applicable DD Form 254. Where classified contract performance will occur on a military/government/contractor installation for 90 days or longer, the contractor shall enter into a long term visitor group security agreement. This agreement, provided by the Government program manager in concert with the SSA, shall be

tailored to specific mission and performance requirements and will include NISPOM and local military/government/contractor security procedures as applicable. As a visitor group operation, contractor access is controlled by the Government. Visitor group security agreements suffice in lieu of SOPs. See Notification of Government Security Activity and Visitor Group Security Agreements Clause (AFFARS 5352.204-9000) in basic contracts.

6.9 Notification of Government Security Activity: Thirty (30) days before the date contractor operations will begin on the military/government installation, the contractor shall furnish the SSA at the performance location all information required by the clause, Notification of Government Security Activity (AFFARS 5352.204-9000). The contractor shall contact the SSA identified in Item 13 of the DD Form 254 for assistance in obtaining the address of the applicable SSA for the performance location.

6.10 Contractor Credentials and Vehicle Passes: For contract performance on a military/government/contractor installation, the contractor shall comply with local procedures provided by the SSA to obtain contractor credentials and vehicles passes.

6.11 Unescorted Entry Authorizations: To obtain unescorted entry authorizations into controlled or restricted areas, the contractor shall comply with local procedures provided by the SSA. Forms accomplished to obtain such entry must be certified by the SSA to ensure the individual requiring unescorted entrance has a personnel security clearance or a favorable background investigation.

6.12 Counterintelligence Awareness Briefing: The contractor shall comply with the military/government/contractor installation's Counterintelligence Awareness Program. Contractor personnel shall report to an appropriate authority any information or circumstances of which they are aware that may pose a threat to the security of DoD personnel, contractor personnel, resources, and classified or unclassified defense information. Contractor employees shall be briefed on this requirement by their immediate supervisor upon initial on-base assignment.

6.13 Crime Prevention Program: While performing on a military installation, the contractor shall adhere to the installation's Crime Prevention Program.

6.14 Privacy Act: Work under this contract requires that personnel have access to Privacy Act Information. Personnel shall adhere to the Privacy Act, Title 5 of the U.S. Code, Section 552a and applicable agency rules and regulations.

## **7.0 DISTRIBUTION STATEMENT E:**

7.1 The Contractor shall distribute all information generated from this PWS in accordance with the following distribution statement: Distribution authorized to DoD Components only (Administrative / Operational Use) (10 January 2013). Other requests shall be referred to GSA.

## **8.0 AT/OPSEC REQUIREMENTS:**

8.1 Contractor employees and all associated subcontractors' employees requiring access to Army installations, facilities and controlled access areas shall complete AT Level I awareness training

within 14 calendar days after contract start date or the effective date of incorporation of this requirement into the contract, whichever is applicable. AT level I awareness training is available at the following website: <https://atlevel1.dtic.mil/at>. The contractor shall submit certificates of completion for each affected contractor employee and subcontractor employee to the COR within seven calendar days after completion of training by all employees and subcontractor personnel. This includes new contractor employees as they are assigned.

8.2 Contractor employees and all associated subcontractor employees shall comply with applicable installation, facility and area commander installation / facility access and local security policies and procedures (provided by the COR as GFI at contract start date or effective date of incorporation of this requirement into the contract, whichever is applicable) such as wearing of ID Badges, etc. The contractor shall also provide all information locally required for background checks to meet installation access requirements to be accomplished by the installation Provost Marshal Office, Director of Emergency Services or Security Office. Contractor workforce must comply with all personal identity verification requirements as requested by the COR based on DOD, HQDA and/or local policy. In addition, should the Force Protection Condition (FPCON) at any individual facility or installation change, the COR may require changes in contractor security matters or processes. During FPCON Charlie and Delta and other required postures such as a Lockdown, Shelter In Place or Evacuation, contractor employees will resume work as soon as possible after the FPCON has been lowered or the posture returned to normal operations. This pertains to real situations and exercises.

8.3 The Contractor and all associated subcontractors shall ensure that all their employees participate in local training as required by the COR based on the local Anti-Terrorism Officer (ATO) requirements, such as local iWatch training, to inform employees of the types of behavior to look out for and instruct employees to report suspicious activity to the COR.

8.4 The Contractor and all associated subcontractors shall ensure that all local clearance procedures (i.e. return of ID badges provided by the COR as GFI at contract start date or effective date of incorporation of this requirement into the contract, whichever is applicable) are followed for departing contractor employees and sub-contractor employees.

8.5 US-based contractor employees and associated subcontractor employees who will perform work OCONUS will receive area of responsibility (AOR) specific AT awareness training as directed by AR 525-13 and meet all country clearance requirements per the Personnel Policy Guidance (PPG) and local deployment requirements and documentation. The COR will provide information (required training, country clearance requirements and local deployment requirements / documentation) as GFI at contract start date or effective date of incorporation of this requirement into the contract, whichever is applicable.

8.6 Contractor employees and associated subcontractor employees, who are authorized to accompany US Armed Forces deployed outside the US in contingency operations; humanitarian or peacekeeping operations; or other military operations or exercises, when designated by the combatant commander, shall comply with local AT / OPSEC policies. These policies include required compliance with laws and regulations, pre-deployment requirements, required training (per combatant command guidance), personnel data requirements to address before deployment,

and required documentation. The COR will provide these policies as GFI at contract start date or effective date of incorporation of this requirement into the contract, whichever is applicable.

8.7 Non-local national (not citizens of the foreign country of performance or delivery) contractor employees and associated subcontractor employees who are required to provide performance or delivery in a foreign country are to comply with country and theater clearance requirements and allow the combatant commander to exercise oversight to ensure the contractor's compliance with combatant commander and subordinate task force commander policies and directives. The COR will provide this information (requirements, policies and directives) as GFI at contract start date or effective date of incorporation of this requirement into the contract, whichever is applicable.

8.8 Contractors and all associated sub-contractors who will handle or have access to Classified Information are to be directed to analyze FAR 52.204-2, Security Requirements. This clause involves access to information classified "Confidential," "Secret," or "Top Secret" and requires contractors to comply with: The Security Agreement (DD Form 441), including the National Industrial Security Program Operating Manual (DoD 5220.22-M); and any revisions to DOD 5220.22-M, notice of which is to be provided by the COR as GFI at contract start date or effective date of incorporation of this requirement into the contract, whichever is applicable.

8.9 Contractor personnel and associated sub-contractor personnel who require access to Government Information Systems must successfully complete the DOD Information Assurance Awareness training, and all other mandatory IA training / forms, which are required by the Government Organization(s) that controls the system(s) that the Contractor requires access to, before accessing these Government information system(s). The DOD Information Assurance Awareness training must be completed annually thereafter. The COR will provide the Contractor with the specific requirement(s) that must be met for access to these systems as GFI at contract start date or effective date of incorporation of this requirement into the contract, whichever is applicable.

## **9.0 GOVERNMENT POINTS OF CONTACT AND CONTRACT MANAGEMENT:**

### **9.1 Additional Points of Contact:**

#### **Contracting Officer (CO):**

Aaron Young  
GSA FAS AAS FEDSIM (QF0B)  
1800 F Street, NW  
Washington, D.C. 20405  
Telephone: (703) 603-8217  
Email: aaron.young@gsa.gov

#### **Contracting Officer's Representative:**

Kareem Jarrett  
GSA FAS AAS FEDSIM (QF0B)  
1800 F Street, NW  
Washington, D.C. 20405  
Telephone: (202) 227-9804  
Email: kareem.jarrett@gsa.gov

#### **Technical Point of Contact:**

John Audia  
RSC-NCR TPOC  
22202 Crystal Drive, Suite 900  
Arlington, VA 22202-0000  
Telephone: 619-709-0975  
E-mail: john.audia@nps.edu

**10. Other Direct Costs (ODCs):** The contractor shall purchase ODC/materials as required and/or as requested. All necessary purchases shall be pre-approved by the GTM and CO prior to purchase.